Journal of Contemporary Criminal Justice
1–22

DOI: 10.1177/1043986217699100
journals.sagepub.com/home/ccj
SAGE

Exploring the Subculture of Ideologically Motivated Cyber-Attackers

Thomas J. Holt[1], Joshua D. Freilich[2], and Steven M. Chermak[1]

Abstract

Research on physical, that is, violent, terror attacks and extremism has increased dramatically over the last decade. The growth of the Internet and computer technology has also led to concern over the use of cyberattacks by ideologically motivated offenders to cause harm and further their political and social agendas. There is, however, a lack of empirical research on cyber-attackers limiting our knowledge of the factors that affect their behavior. This study addresses this empirical gap through a qualitative analysis of 10 interviews conducted with ideologically motivated Turkish computer hackers. The findings demonstrated that Turkish hackers motivated by an ideological agenda reflected the larger values of the hacker subculture, though the targets for their attacks were shaped directly by religious or political beliefs. We conclude by discussing in depth our findings and implications for counterterror and cybersecurity policy and practice.

Keywords

cybercrime, cyberterror, computer hacking, hacktivism, extremism

Research on terrorism has increased dramatically following 9/11, with a substantive focus on the pathways that lead individuals to accept a radical ideology and engage in acts of physical violence (Bakker, 2006; Borum, 2011a, 2011b; Brenner, 2009; Freilich, Chermak, Belli, Gruenewald, & Parkin, 2014; Hamm, 2007; Kunkle, 2012; McCauley & Moskalenko, 2011; Monahan, 2012; Sageman, 2004; Silber, 2011; Simi

[1]Michigan State University, East Lansing, USA
[2]John Jay College of Criminal Justice, New York, NY, USA

Corresponding Author:
Thomas J. Holt, School of Criminal Justice, Michigan State University, East Lansing, MI, USA.
Email: holtt@msu.edu

& Futrell, 2010; Stern, 2003). There is, however, far less research on the issue of ideologically motivated attacks in cyberspace, and their perceptions of the skills and strategies necessary for building a capacity to carry out these attacks (Denning, 2010; Holt, 2012; Holt & Kilger, 2012).

The growth of the Internet, mobile phones, and inexpensive computing devices affords more than just communications capabilities, as virtually all aspects of finance, power, water, and sewer grid management as well as government and military operations depend on the Internet to function (Andress & Winterfeld, 2013; Holt & Bossler, 2016). All these resources are susceptible to compromise through various forms of cyber-attack, such as the distribution of malicious software to affect the functionality of computer systems. Alternatively, techniques like denial of service (DOS) attacks can be used to knock systems offline, rendering them useless to others which then causes inconvenience and economic harm (Andress & Winterfeld, 2013). Even simple web defacements, where the primary content of a website is replaced by images and text selected by the attacker, serve as a venue for political and ideological expression (Brenner, 2009; Holt & Kilger, 2012; Woo, Kim, & Dominick, 2004).

There have been few empirical investigations of cyberattacks by extremist groups and ideologically driven actors (for exceptions, see Holt & Bolden, 2014; Holt & Kilger, 2012; Holt, Kilger, Chiang, & Yang, 2017; Torres-Soriano, 2016), leading to difficulty in developing counterterror policy and prevention strategies related to ideologically motivated cyber-attackers (Brenner, 2009; Denning, 2010). One reason for the empirical gap on cyber-terror, and ideologically motivated online crimes generally, is the narrow focus of most terrorism definitions developed by researchers and nations alike. Definitions of terrorism have changed over time, leading to a range of frameworks with different inclusion criteria (Hoffman, 1998; Weinberg, Pedhazur, & Hirsch-Hoefler, 2004). Importantly though, almost all definitions require terrorist acts to be ideologically motivated crimes committed by nonstate actors that use "*force or violence*" (Freilich, Chermak, & Simone, 2009; Hoffman, 1998).

As an attack against computer systems via the Internet usually does not involve force or violence as traditionally recognized in physical acts of terrorism, they are excluded from definitions of terror. The United States does not have a federal legal definition for cyber-terror in existing criminal codes, but instead folds incidents under existing laws pertaining to cybercrime (Holt, Bossler, & Seigfried-Spellar, 2015). The same is true with respect to terrorism databases and studies which normally exclude financial or cybercrimes and Internet-related crimes committed by extremists even if they are ideologically motivated simply because they are nonviolent offenses (e.g. LaFree & Dugan, 2007). Similarly, ideologically motivated cyberattacks are largely kept out of the popular press as organizations tend to conceal that they have experienced a breach or hack until months or years after the fact (Andress & Winterfeld, 2013; Holt & Bossler, 2016).

Although physical violence is largely absent from cyberattacks, they have the potential to cause substantial economic harm especially if an attack prevents consumers from accessing financial systems or businesses from engaging in commerce (Holt & Bossler, 2016). Similarly, the disruptive power of a cyber-attack against a major target, such as

electrical grids or government resources, could cause fear in the larger population that they may be subject to repeated compromise or further harm (e.g., Holt, 2012). In this respect, ideologically motivated cyberattacks may have more in common with traditional terror despite the absence of real-world violence. This may account for the fact that both government officials as well as state and local law enforcement consider cyberterror attacks to be a real threat with a potential severity second only to a physical terror attack (Holt, Bossler, & Fitzgerald, 2010; Holt, Burruss, & Bossler, 2015).

As a result, there is a need to understand the extent to which ideological motivations influence the targets and practices of individuals interested in cyberattacks against government and industry targets. If politically driven hackers significantly differ from the larger hacker community, there may be a need to tailor policy responses to affect these actors and mitigate their behaviors in addition to the current strategies in place to combat cybercrime as a whole (Brenner, 2009; Holt & Bossler, 2016). Existing examinations of political or ideologically driven cyberattacks and extremist behaviors have mostly been theoretical with occasional case studies regarding attacks (Denning, 2010; Holt & Bolden, 2014). This creates a substantive dark figure of ideological crimes that could be addressed through more rigorous counting schema and definitions for behavior.

This study attempts to address this research gap through a qualitative assessment of historical data collected from a sample of Turkish computer hackers involved in ideologically motivated cyberattacks targeting nations around the world (Andress & Winterfeld, 2013; Denning, 2010). The analysis compares their perspectives against existing research on the hacker subculture in the United States and Europe. In addition, we consider how political and religious ideologies shape perceptions and justifications of hackers within this community. The implications of this study for our understanding of cyberterrorism, ideologically motivated cyberattacks, the contextual use of technology, and, importantly, how it may impact violent terrorism within extremist movements are considered in detail.

Ideological Extremism and Cyberattacks

Although many assume that cyberattacks are committed by hackers interested in money or information (Franklin, Perrig, Paxson, & Savage, 2007; Kilger, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011), there is increasing evidence that ideologically motivated groups also engage in computer hacking and attacks against networked computer systems (Denning, 2010; Holt & Kilger, 2012). Most nations depend on the Internet and networked computer systems to manage financial, governmental, and industrial business, as well as maintain critical infrastructure, leading extremist groups to recognize the value in targeting these resources (Andress & Winterfeld, 2013; Britz, 2015; Denning, 2010). For instance, Mohammad Bin Ahmad As-Sālim's treatise *39 Ways to Serve and Participate in Jihâd* discusses how an electronic jihad could disrupt the West through targeted hacks of American websites, and other resources seen as anti-Jihad, modernist, or secular in orientation (Denning, 2010; Leyden, 2007).

An additional value of cyberattacks is that they provide a venue for asymmetric conflict: Attackers can spend minimal financial resources and man-hours to produce attacks with a high probability of success that have a low risk of detection or arrest (Brenner, 2009; Denning, 2010). These conditions have led to the formation of loose associations of hacker groups referred to as the e-Jihad interested in engaging in cyberattacks against the West (Denning, 2010; Ulph, 2006). Ardit Ferizi was detained in Malaysia in October 2015, for instance, for compromising U.S. computer systems to obtain personal information on 1,300 military and federal employees. Ferizi then provided this information to Islamic State of Iraq and the Levant (ISIS) members for further use (Perez, Shoichet, & Bruer, 2015). Similarly, Tariq al-Daour, Waseem Mughal, and Younes Tsouli acquired credit and debit card numbers through phishing and malware from 2003 to 2005. They used this information to purchase equipment for jihadists in the field, host videos and forums supporting jihadist movements, and provide manuals on hacking methods (Krebs, 2007).

A number of web forums and hacker groups also regularly promote the use of hacks and cyberattacks against the West (Torres-Soriano, 2016). For instance, the al-Farouq forum ran a site-subsection where members encouraged targeting Western websites for electronic jihad through the use of a downloadable library of tools and tutorials to complete an attack (Denning 2010; Pool, 2005). The al-Jinan hacker forum also created and offered a free download of a DoS tool called Electronic Jihad and awarded electronic medals to the forum users most effective in targeting and taking down websites that were seen as anti-Islamic (Bakier, 2007; Torres-Soriano, 2016).

Hackers and Hacker Subculture

Although extremist groups recognize the value in cyberattacks (Holt & Bolden, 2014; Torres-Soriano, 2016), it is unknown how their motives and beliefs compare with the larger computer hacker community. Hacking is a skill that can be applied for either legitimate security purposes or malicious, criminal endeavors (Franklin et al., 2007; Holt & Lampke, 2010; Jordan & Taylor, 1998; Motoyama et al., 2011; Steinmetz, 2015). In fact, many of the same basic principles and techniques are applied regardless of an individual's motivations (Holt, 2007).

There is a need to understand the extent to which ideologically motivated hackers express the same beliefs as those motivated by money, status, or security reasons (e.g., Holt & Bolden, 2014). Specifically, do they only hack to achieve a political, religious, or ideological agenda? Or, do they hack for entertainment, education, or other reasons? Or is it some combination of different motivations? It is possible that cyberattackers are similar to violent terrorists who commit crimes for a variety of ideological and nonideological reasons (Martin & Augustus, 2016). For instance, the United States Extremist Crime Database (ECDB) includes more than 1,800 domestic terrorism incidents/schemes and more than 3,500 offenders (Freilich & Chermak, 2016). One unique characteristic of this database is that it includes both ideologically and non-ideologically motivated crimes committed by extremists in the United States, including over 850 nonviolent financial schemes (Freilich & Chermak, 2016). Analyses of these data

indicate that the extremists involved in these financial schemes participated for a variety of reasons, sometimes to further a political ideology and other times to simply make money (Freilich et al., 2014).

Here, we investigate if extremists committing nonviolent cyberattacks are also motivated by a combination of both ideological and nonideological influences. In other words, it is essential to understand the extent to which a broader series of beliefs or values exist and influence the perceptions of hackers generally. Sociological and criminological inquiries on the U.S. and European hacking subcultures suggest that computer hackers' behaviors are guided by a series of interconnected norms, values, and beliefs (Holt, 2007; Jordan & Taylor, 1998; Loper, 2000; Meyer, 1989; Steinmetz, 2015; Taylor, 1999; Thomas, 2002). Hackers usually emphasize the need to understand technology in profound ways, and apply that knowledge so that computer hardware and software operate in ways they were not initially designed to perform (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2015; Taylor, 1999).

As a consequence, knowledge and mastery of technology play a significant role in hacker subcultures (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999). Hackers spend a significant amount of time learning about technology and how devices work at deep levels. This fuels the importance of technological mastery in hacker subculture, exhibited either through social exchanges in forums and social media (Holt, 2007; Meyer, 1989; Steinmetz, 2015; Thomas, 2002) or through direct recognition of successful attacks (Holt, 2013; Meyer, 1989). Various forums enable individuals to report their completion of hacks and thus gain social recognition (Holt, Bossler, & Seigfried-Spellar, 2015; Woo et al., 2004). In fact, the web defacement repository Zone-H operates on the basis of self-disclosure of completed attacks which are attributed to a specific hacker (Zone-H, 2016).

While hackers may use their skills to engage in criminal or ethical hacks, their actions may not have a substantial impact on their construction of a deviant identity, even though their targets may feel the attacker is an obvious criminal (Furnell, 2002; Holt, 2010). Members of the hacker community use different terms to differentiate themselves from others on the basis of the ethics of their activities, such as black hat or white hat hackers which acknowledges the use of malicious or ethical applications of hacking (Furnell, 2002; Holt, 2010). The generally illicit nature of hacking may, however, influence the importance of secrecy historically observed in the hacker subcultures (Holt, 2007; Jordan & Taylor, 1998; Meyer, 1989).

To that end, hackers typically use handles or nicknames in online and offline environments to hide their real identity (Holt, 2007; Jordan & Taylor, 1998; Meyer, 1989; Taylor, 1999). Successful hackers attribute the action to their handle, leading to a desire to brag and share accumulated knowledge with others (Taylor, 1999; Thomas, 2002). Taking responsibility for specific hacks can not only help individuals gain status within the hacker community, but also increases their risk of law enforcement detection (Taylor, 1999). To minimize their likelihood of arrest, hackers may operate in closed communities and only acknowledge their attacks via defacements or in the code of malicious software (Holt, Smirnova, Chua, & Copes, 2015). Similarly, hackers who provide tutorials and information on how to hack may also indicate that the

knowledge they provide is only meant to test the security of a computer or network that an individual owns or operates (see Holt, 2007; Hutchings & Clayton, 2016; Hutchings & Holt, 2014). Thus, hackers operate in a difficult space between sharing information and keeping certain knowledge private to maintain some degree of plausible deniability and to minimize their risk of liability.

There is, however, limited research that examines how ideologically motivated offenders view cyberattacks. Hackers are driven in part by their beliefs (Denning, 2010; Holt & Kilger, 2012; Kilger, 2010; Turgeman-Goldschmidt, 2008); thus, it is imperative that researchers investigate if political motivations separate such hackers from the larger subculture (see Holt & Bolden, 2014). It is unknown if ideological motivations shape the experiences of hackers or produce differences in views on hacking generally.

If differences exist, there may be a need to identify unique policies to sanction cyber-attackers in much the same way as terrorists who engage in physical attacks. There is a clear need to identify the relationship between cyberattacks and physical violent actions. For instance, both hackers and individual terrorists learn methods and messaging techniques from one another (Bloom, 2005; Hamm, 2007; McCauley & Moskalenko, 2011).

At the same time, differences in attacker behavior on the basis of motivation require changes to shape technical cybersecurity in practice to minimize threats from economically driven cyber-attackers as well as those motivated by a political or religious ideology (Andress & Winterfeld, 2013; Brenner, 2009). There is, however, generally little research examining the ways that ideologically motivated cyber-attackers view their activities or the extent to which they correspond or differ from that of the larger body of attackers generally (e.g., Holt & Bolden, 2014). Thus, this study begins to address these questions through a qualitative analysis of a series of interviews with Turkish computer hackers who regularly engage in ideologically motivated hacks.

Data and Method

Our data consist of a series of 10 in-depth interviews conducted via email or instant messaging with prominent hackers who self-identified as being Turkish and involved in the hacker subculture within the country. Turkish hackers were purposefully targeted because of their general involvement in political and ideologically motivated hacks, including a series of web defacements against thousands of websites that published a cartoon featuring an image of the prophet Mohammed with a bomb in his turban (Denning, 2010; Ward, 2006). The interest among Turkish hackers in targeting websites on the basis of their ideological beliefs provided an ideal sample to begin understanding the role of motive in their experience of computer hacking and cyberattacks in general.

Interviews were collected from June through August of 2008 and probed individuals' experiences and impressions of the normative orders of hacker subculture online and offline. Respondents were asked to describe their experiences with hacking, interactions with other hackers both online and offline, and their opinions on the Turkish hacker

subculture. Interviewees were identified and contacted through two fieldworkers who served as participant recruiters with significant status among Turkish hackers. The individuals had direct access to prominent hackers through their role at a cybersecurity incident reporting organization. The fieldworkers contacted 12 well-known hackers via email, inviting them to participate in this study, and 10 agreed to participate.

Individuals who responded to the solicitation were sent a copy of the interview protocol, allowing respondents to complete the instrument at their leisure. The protocol included a series of open-ended primary questions with probing queries that served to gain more information from respondents in much the same way as a traditional face-to-face interview (e.g., Holt, 2010; Silverman, 2013). Questions included the respondents' personal experiences with technology; their first, last, and most successful hacks; how they came to be involved in hacking; and their thoughts on what constitutes a hacker and why. Respondents were given the option to complete the instrument in either Turkish or English. Eight of the interviews were completed in Turkish, which were professionally translated by a certified translator to ensure accurate and reliable results (see also Holt, 2010; Holt, Smirnova, Chua & Copes, 2015). Respondents could be asked follow-up questions or clarification on their comments via email to ensure accuracy.

These data provide valuable insights on a rarely examined phenomenon: ideologically motivated cyber-attackers. The small sample of interviewees does not, however, provide a generalizable sample to all attacker populations around the world. At the same time, there are no real estimates as to the number of ideologically motivated hackers around the globe at any point in time. Furthermore, the data are temporally bound, making it an open question as to how applicable it is to hackers almost a decade later.

Despite these limitations, there is virtually no empirical data assessing ideologically motivated hacking (Jordan & Taylor, 2004). The fact that all the participants in this sample engaged in at least one ideologically motivated hack ensured that they served as a convenient, yet purposive sample of hackers. Thus, these data can serve as a historical case study to begin the process of understanding the relationship between political motivation and experience as a hacker generally. In addition, the findings can shed light on unresolved questions regarding the practices of ideologically motivated actors online and offline, and provide an agenda for future research to address.

To assess the subculture of hacking and the role of motive within attacks generally, the data were analyzed through the concept of "normative order" (Herbert, 1998, p. 347). This is a "set of generalized rules and common practices oriented around a common value" (Herbert, 1998, p. 347). An order "provide[s] guidelines and justifications" for behavior, demonstrating how subcultural membership impacts actions (Herbert, 1998, p. 347). This gives a dynamic view of culture, recognizing that individual behavior can stem from individual decisions as well as through adherence to subcultural values. Normative orders also provide for the identification of informal rules considered important by members of the subculture because of the values they uphold. Furthermore, this frame allows the researcher to recognize conflicts in the subculture based on the presence of contradicting orders (Herbert, 1998).

Herbert (1998) provides little guidance, however, on how to actually measure or identify normative orders. His results were generated from ethnographic observations of police in a variety of settings. As such, these interviews were printed and analyzed by hand using the three-stage inductive analysis methodology derived from grounded theory (Corbin & Strauss, 2007). This useful coding and analysis scheme permits the researcher to develop a thorough, well-integrated examination of any social phenomena. Any concepts found within the data must be identified multiple times through comparisons to identify any similarities (Corbin & Strauss, 2007). Findings are thus validated by their repeated appearances or absences in the data, ensuring they are derived and grounded in the data.

For this analysis, normative orders are inductively derived from the repeated appearance of specific actions, rules, or ideas in the data similar to prior analyses of online subcultures (Blevins & Holt, 2009; Holt, 2007). The value of these concepts is generated from positive or negative comments of the respondents. In turn, theoretical links between these concepts are derived from the data to highlight the value or "normative order" that structures the behavior of hackers.

Findings

These methods are used to critically explore the interplay between ideological motivation and the hacker subculture among a sample of Turkish computer hackers. From this analysis, the experiences of ideologically motivated hackers were shaped by four normative orders including technology, knowledge, commitment, and the mission. These orders generate justifications for behavior, affect attitudes toward hacking, and structure identity and status within the subculture. The contours and connections of these normative orders are examined through the use of quotes from the interviewees when appropriate.

Technology

One primary issue that emerged in the course of the interviews was technology's role in the formation of a hacker identity, consistent with the larger research on the hacker subculture generally (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2015; Taylor, 1999). Six of the Turkish hackers interviewed indicated that they became interested in technology either at a young age or when they were given access to computers. For instance, Blue Crown stated,

> I got to know computers when I was a child. Technology has always been an area of interest for me. I try to follow anything about technology every day. My interest grew as I dealt with computers and fumbled around.

Similarly, Ghost 61 wrote, "I didn't go to school, I was in front of my computer all the time. I didn't study, I hacked. I didn't go out, I hacked. I worked on it a lot to learn new things."

Given the differences in access to technology, a proportion of interviewees also discussed the role of Internet cafes in gaining exposure to computers and the Internet. In the early 2000s, home Internet access in Turkey was expensive leading many to opt for more affordable pay-for-use experiences in Internet cafes. Crazy King exemplified this notion stating,

> going to internet cafes in 2000 is the main reason for this and in the forums I was what could be done with a computer and I started to get interested in it . . . The love I feel for technology.

Also, Amen indicated that he was able to work out a mutually beneficial relationship with an Internet cafe operator stating,

> I have been interested in computers for 7 years. In internet cafes, while everybody else were playing games I was working on the automation system for the café. In return, I was not paying any money for my usage of the computers.

Thus, Turkish hackers reflect the larger emphasis on gaining access to technology through any means necessary in the larger hacker subculture (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999). The more exposure individuals could generate, the more their technological interests grew.

Knowledge

The interviewees also stressed that the importance of technological exposure was intertwined with the need to understand how computer hardware and software operated to hack. This view is supportive of the larger norm of knowledge within the hacker subculture (Holt, 2007; Jordan & Taylor, 1998; Meyer, 1989; Steinmetz, 2015; Taylor, 1999), as evident by the fact that many interviewees indicated the value of learning and applying their own knowledge to become technologically proficient. For instance, Agd_Scorp stated that he learned to hack largely on his own through "trial and error, and some documents on the internet. But trial and error is the best method." The Bekir echoed this sentiment saying,

> In the beginning I looked at illustrated explanations on the web and acted accordingly, but they were not sufficient for me. I wanted to learn how this was done, how these were provided and I fiddled about with them a lot until they broke down.

To cultivate knowledge, many of the hackers interviewed stated that they read tutorials posted by members of the Turkish subculture. A number of hackers also learned from videos posted on YouTube and other sites. For instance, Axe said he felt like a hacker when "It was the time to apply what I saw in the videos I watched." The hacker Iscorpitx was actually a content generator for Turkish hackers stating,

> In general, I like sharing the things I do after a while. A lot of videos I recorded while defacing online were very useful for a lot of people who are on the security side of this

> business . . . I got root authorization in a hosting of NetSol where approximately 300,000 web sites exist. But I didn't deface any of its websites. I only recorded them on video to prove on my own site how insecure these systems are. ☺ . . . Of course, you can't be skilled and informed in every subject. Everybody needs help.

Others participated in forums with other Turks as a means to learn. Crazy King stated, "I can say that this experience [visiting a forum] had a big influence on me: practicing subjects that I didn't know or I forgot, learning better methods, etc." The Bekir shared this view stating,

> There was a web forum, which was created by a very close friend of mine. I was in that forum for 2-3 years and it was quite nice . . . I learned a lot of things at that site and helped them to learn a lot of things as well.

Turkish hackers also indicated that they were able to learn through direct and indirect mentoring from others. While previous research on the hacker subculture recognizes the role of peers in the development of interest in hacking (Holt, 2013; Jordan & Taylor, 1998; Steinmetz, 2015), few have found evidence of hackers directly training and educating others. Ghost 61 suggested he was initially interested in hacking on his own, and garnered skill by watching "a lot of hacking videos and I learned together with the friends who helped." Blue Crown, however, suggested he became involved in hacking as a direct result of engagement with others in the community stating,

> I had some interest in hacking but I wasn't planning to get involved in this business. One day, an interview with a hacking group on television caught my attention . . . I turned on my computer and immediately started to browse. I met a hacker with a code name [removed] in [a major Turkish hacker group]. I owe him/her a lot . . . I thought I couldn't do anything but s/he helped me and taught me a few things. I learned quickly thanks to the interest I had.

As a result, Turkish hackers may be unique compared with the larger subcultural emphasis on self-learning (e.g., Holt, 2007; Jordan & Taylor, 1998; Meyer, 1989).

The cultivation of knowledge had a direct influence on the capabilities of Turkish hackers as noted in various studies of the hacker community generally (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2015; Taylor, 1999). The diversity of operating systems, programming languages, hardware, and software used by individuals every day led to some specialization in attack techniques and knowledge within the Turkish community. Some individuals used specialized tools or scripts to help them hack, such as Agd_Scorp who preferred to "make sql injection attacks. So I only use an internet browser… I don't like using tools. Of course sometimes they help you to shorten your hack time." Others like Amen would use whatever tools made the most sense to facilitate an attack using whatever programming skills necessary stating, "ASP, SQL union, update, Linux root, etc. It is easy to use if you know what you are doing. Of course, I generally use my own tools."

The hackers interviewed also explained that the Turkish community was relatively tight-knit, sharing both attack tools and target information with others. Blue Crown noted, "If Turkish hackers find a hole/weak point, they share this after exploiting it. This is a bad characteristic of Turkish hackers." Crazy King also noted a general preference for Turkish-made malware and tools in the larger hacker community in Turkey:

> In general we [Turkish hackers] use a keylogger and trojan in personal and special/private attacks. We use bots to overstrain the server and put it out of operation in transcendent systems . . . They are the sources that we develop ourselves and belong to us.

Those with greater knowledge have more opportunities and avenues for attack, while individuals with less understanding are limited to certain targets or attack venues.

This was exemplified in a comment from Iscorpitx, who wrote,

> The expertise areas of hacker groups are different as well. If a hacker wants to harm a site where s/he has an obsession, s/he will. If s/he can't, s/he can get help. If s/he can't do anything, s/he can stop the publication of the website using a Ddos attack. But if s/he wants, s/he can cause harm. The ones who have enough knowledge and information can manage this; otherwise it is very difficult. The ones who don't have enough knowledge can't get help as well.

Blue Crown echoed this sentiment, noting that his abilities allowed him to use free hacking tools that he could alter to make them more effective:

> When I'm going to perform a personal hack, I need an undetected keylogger or trojan. Some trojans are subject to payment and some of them are free of charge. The only difference between these two trojan types is that trojans subject to payment are undetectable (they can't be caught). I can make a free of charge trojan "undetectable" by using some Crypt programs. Friends who develop the Crypter work for this. They usually use well-known and existing weak points/holes.

These findings demonstrate that Turkish hackers have various skills and abilities, though they differ from the larger subculture in the extent to which their skills are cultivated independently or through direct engagement with others (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999).

Commitment

Turkish hackers recognized that to develop into full-fledged hackers, they had to apply their knowledge in the real-world. The more time a person hacks, the more their knowledge and ability improves (Holt, 2007; Taylor, 1999). The ways that individuals demonstrate their knowledge through hacking can lead others to judge them on their abilities (Holt, 2007; Jordan & Taylor, 1998; Taylor, 1999). For instance, the Bekir felt that the frequency with which a person engages in hacking may not be a point of derision but rather a means to understand their potential and skill. He indicated,

> there are hackers who hack web sites that have weak points; they [less skilled hackers] make fun of these hackers by saying "do you have to hack every site that has a weak point?" However, the more hacks this person performs, the better s/he gets information about different systems and passes different types of security systems. It is a nice thing for them to develop themselves. There are targeted hackers and malevolent ones; everybody has different opinions to defend.

In this respect, Turkish hackers share much in common with the larger hacker subculture where those who engage in seemingly random attacks facilitated by scripts are viewed as unskilled (Holt, 2010; Jordan & Taylor, 1998). Such hackers are usually derogatorily referred to as script kiddies due to their dependence on automated attack tools to hack. Agd_Scorp commented on this issue as well noting, "There are many experienced coders and crackers in turkey, but many of defacers are only script kiddies. Only a few of defacers really makes their own ways to hack a site."

The Bekir also noted that Turkish hackers could be adversarial with one another, though skill had some influence on how others viewed you. He stated,

> Whether you are skilled or not, you get a dressing down from the ones who are not that skilled ☺ In other words, whatever skills you have, that person teases/annoys/provokes you, considering you're virtual. Turkish hackers give importance and respect to big hacks. They are respectful of knowledge but if this is among the skilled/expert ones.

The noted importance of long-term, applied knowledge was also referenced by five of the interviewees in their definition of what constitutes a hacker (Holt, 2007). Crazy King suggested, "hacker is the faceless/unrecognized one; being a hacker means to hack and access any kind of system whenever and under any circumstance s/he wants to," while Amen suggested a hacker is "someone who reads, explores, and absorbs the minute details." This notion was exemplified by The Bekir stating, "a hacker is a person who isn't aware of sleeping, eating, drinking water, who doesn't have a social life like me . . . When I was dealing with hacking I lost my life, myself, I forgot everything."

In describing the meaning of being a hacker, Iscorpitx also identified the issue of character and ethics which is common in larger discussions of hacking (e.g., Holt, 2007). He wrote,

> the definition of Hacker is very relative. There are many definitions already. A hacker is always perceived as a bad person, thief, burglar, somebody out to harm. But this is directly related to the characters of the people who are performing this job. If they are accessing the systems for their own financial benefit, these groups are called black and illegal. Gray hats, web crackers change the interfaces of the sites if there are holes/weak points in the server. Hackers in white groups have fun by warning only and notify the security sites about the security holes/weak points that they discovered themselves.

Taken as a whole, the Turkish hacker community reflected the larger absence of a single definition for hacking evident in the larger subculture (Holt, 2007, 2010).

Instead, individuals have different views on what makes someone a hacker or how they can be evaluated compared with others.

The Mission

Although many of the comments provided by Turkish hackers were a reflection of the larger norms identified in studies of the hacker subculture (Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2015; Thomas, 2002), ideological and nationalist motivations had a unique influence on their perceptions that deviate from prior research. For instance, the hacker Axe suggested that his definition of a hacker was driven by a combination of perspectives: "a very good understanding and knowledge of the computer world can be categorized as a hacker . . . Being a hacker means to have big targets and a specific mission." For Turkish hackers, the notion of a mission was an important aspect of their targets and general identity beyond being a hacker. Amen demonstrated this idea stating, "everything is for the mission . . . Which other nation is as patriotic as Turks?" Similarly, Ghost 61 believed Turkish hackers to be different from the larger hacker community around the world stating, "everyone does this [hacking] for money and financial benefits, but turkish hackers do it for the flag, for the homeland." Blue Crown felt "Turkish hackers are devoted to their flags, language, and nation."

The role of nationalism was also combined with religion, given that Turkey is a Muslim-majority nation. This was exemplified in a quote from Iscorpitx, indicating the diversity of Turkish hackers:

> Among Turkish hacker groups, we can count Islamic groups, revolutionist groups, groups with ideas supporting Ataturk, nationalist groups, etc. There are very talented and skilled young people . . . But these talents are very rare. They have much respect for their national and moral values.

The notion of mission-based hacking directly influenced the targets Turkish hackers selected to hack as a means to express their ideas and beliefs. Ghost 61 suggested, "I determine it [targets] according to the agenda; usually they are countries like the usa, israel, russia. In other words, enemies of muslims." The Bekir took a similar approach noting,

> I determine my targets in terms of hits. I was working on hacking web sites that were involved in terrorism; if the hacked web site is big then it makes a greater splash, I'm usually working on hacking terrorism sites, etc.

Blue Crown took this concept a step farther explaining that he trained other hackers with a specific purpose stating,

> I have real friends whom I teach hacking personally . . . Except a few (who do this for fun/as a hobby), all of them hack PKK [the Turkish separatist organization]- and pornographic sites that are my targets as well.

In addition, global politics directly influenced the decision-making process of Turkish hackers. The rise of anti-Muslim sentiment in Western nations led some hackers to target resources they viewed as enemies of their faith. For example, Agd_Scorp wrote, "some countries deliberately attacks muslims . . . America is the country which killed the most muslim in the world. And united nations also killed many muslims and innocent people." The Dutch outlet Jyllen Postens's publication of an offensive cartoon of Muhammad also influenced the targeting decision of Turkish hackers. Blue Crown, for example, wrote, "As you know, nearly HALF of the sites with the .dk extension were hacked by Turkish hackers in order to protest the disgusting and dreadful cartoons by Denmark."

Iscorpitx tied these hacks to a different issue involving a bill that was being drafted in France to publicly acknowledge and criminalize the Armenian genocide conducted by Ottoman forces in 1915 through 1917. The Turkish government maintained that this was not an act of genocide, which inflamed tensions between the two countries. As a result, Iscorpitx stated,

> as long as this Armenian bill is brought up to Turkish people as in the past, these hack attacks will grow. The impertinent draft bill prepared by France caused me to leave protesting messages [web defacements] on 43,000 sites. In the bill they stated that Turkish people killed Armenians, people who are against this will be sentenced to prison. In other words, if France (vote hunter of the 20th century) brings such a ridiculous bill, I think the reaction of our people is not that much. They may have done this because they know that we assign great importance to this issue. For example, the cartoon crisis in Denmark (cartoons that affronted Islam). This resulted in huge damage at a lot of sites in Denmark. Not only Turkish hackers attacked, also Arabic hackers did.

The role of a national and religious "mission" had a direct influence on the organizational practices of Turkish hackers. The larger hacking literature suggests most hackers act alone or in small teams of two to three people for the sake of efficiency and secrecy in attacks (e.g., Décary-Hétu & Dupont, 2012; Dupont, Côté, Savine, & Décary-Hétu, 2016; Holt, 2013). In much the same way, Turkish hackers would attempt to compromise as many websites as is possible, but would attribute the attack to a group identity to promote their agenda. Amen noted,

> They form groups. It doesn't take long, it is done quickly. They do not team-up for a single web site. Then somebody comes up and announces that he broke into a site. You check it and it is really broken. But then it becomes a team job, although a single person discovers it usually.

This practice ensured maximum harm across a range of targets in the most efficient way possible. Crazy King explained this idea in detail stating,

> If popular events (like war) are the case, they come together as a team in order to harm the systems with country extensions. Individually they target large systems and work individually in order to leave protesting messages. They do this by telling their common

> actions to each other or with the documents they write in the forums or videos or texts. If there is a very important event involving the world and people, they can immediately come together.

Thus, Turkish hackers may be more selfless in their attack practices to promote their ideological messages to a global audience. Furthermore, the majority of their hacks were driven by their ideological beliefs, and not on garnering a profit or generating a reputation for competency (e.g., Kilger, 2010). This suggests ideologically motivated hackers may differ from hackers with more flexible motivations.

Discussion and Conclusion

Research on physical terror attacks and terrorist groups has expanded dramatically over the last two decades. The growth of the Internet and ubiquity of technology have created a new landscape for terrorist groups to communicate, fundraise, and gather intelligence about targets in near-real time (Britz, 2015; Conway, 2006; Martin & Augustus, 2016). Although various studies have documented the utility of technology for terrorists, few have considered the extent to which ideologically motivated actors commit cyberattacks against industrial and government targets to cause harm (Freilich, Chermak, & Gruenewald, 2015; Holt & Bolden, 2014; Torres-Soriano, 2016). This study attempted to address this gap in the literature through a qualitative investigation of the influence of motivation on the experience of being a hacker within a sample of 10 Turkish hackers.

We found that ideologically motivated hackers share much in common with the larger hacker subculture in terms of the developmental process of becoming a hacker (Holt, 2007, 2010; Jordan & Taylor, 1998; Meyer, 1989; Steinmetz, 2015; Taylor, 1999). The Turkish hackers placed substantial value on their ability to apply technological expertise to manipulate computer hardware and software. They also recognized the importance of individual time commitments to become technologically proficient (Holt, 2007). Similarly, there was some variation in the definitions individuals had for what constitutes a hacker, with terms to refer to individuals on the basis of their skills (Holt, 2010; Jordan & Taylor, 1998).

The primary difference observed between ideologically motivated hackers and the larger subculture lay in the resources they targeted. Regular nonpolitical hackers target systems for personal reasons such as to have fun (Holt, 2007; Jordan & Taylor, 1998), make a profit (Franklin et al., 2007; Hutchings & Holt, 2014; Motoyama et al., 2011), or better understand the function of a specific piece of hardware or software (Steinmetz, 2015). Conversely, Turkish hackers appear motivated by an ideological belief system that drives their actions and targeting to promote their interests. They appeared either to target specific websites because they were at odds with their religious or political beliefs, or to generate large amounts of attention to their cause. Furthermore, Turkish hackers would perform any sort of attack if it suited their needs, though there was some evidence of attack specialization which may lead to relatively tailored and consistent attack patterns.

Taken as a whole, these findings demonstrate that there may be no way to immediately separate ideologically motivated hackers from the larger population of hackers as a whole. Their shared values generally reflect those of the hacker subculture, making it difficult to identify or tailor deterrence strategies to these actors on the basis of criminal sanctions alone (Hutchings & Clayton, 2016; Maimon, Alper, Sobesto, & Cukier, 2014; Newman & Clarke, 2003). The international nature of cybercrime adds to this challenge, as the lack of extradition relationships between certain countries makes it difficult to deter hacks, as evident in Russian or Chinese hackers affecting U.S. targets (Brenner, 2009; Holt & Bossler, 2016). Furthermore, their ideological motivation may make it difficult to keep cause-based hackers from completing attacks because of their perception of the superiority or righteousness of their ideals.

Instead, there may be greater benefit in developing technological solutions and postures to mitigate the effectiveness of attacks performed by ideologically motivated hackers. The findings of this analysis suggest attackers may be more inclined to target public-facing resources such as websites operated by government or industry rather than internal databases or sensitive information. This is consistent with situational crime prevention (SCP) research on violent terrorism which maintains that not all targets are equally at risk, requiring the development of instruments to identify the more vulnerable/at risk infrastructure and resources (Freilich & Newman, 2009; Gruenewald, Allison-Gruenewald, & Klein, 2015; Newman & Clarke, 2003).

As web-facing resources are primarily used by consumers and citizens, a successful attack would likely be noticed by the general public. In turn, this could cause the victim organizations to be embarrassed, while simultaneously drawing attention to the attackers' cause (Denning, 2010; Woo et al., 2004). These spaces may also have a generally weaker security posture due to the need to keep resources readily accessible to users at all times, coupled with the fact that many businesses may depend on outsourcing website maintenance and security to third party hosting companies (Anderson, Fleizach, Savage, & Voelker, 2007; Canali, Balzarotti, & Francillon, 2013).

Thus, governments and organizations must leverage their security dollars and resources to improve the security of website management to proactively reduce the likelihood that an attack will be successful at the outset. One effective strategy that many organizations could use to thwart hacking is to again borrow from SCP's arguments to harden virtual targets from compromise (Holt & Bossler, 2016; Newman & Clarke, 2003). Implementing security updates and patches frequently, along with increased use of hard passwords and system configurations that are customized to differ from factory standards, may help to increase the difficulty in compromising a resource (Holt & Bossler, 2016; Newman & Clarke, 2003). As ideologically motivated attackers are unlikely to be completely deterred from an attack, such steps may at least allow computer users to intentionally displace an attacker to other targets for a period of time and mitigate harm, as some SCP proponents have noted.

It is important to emphasize that in cases involving industry, it is the private sector that may be best able to respond and to prevent these types of attacks (Holt & Bossler, 2016). The formal criminal justice system has traditionally been seen as responsible for both apprehending and preventing illegal activity, though mitigation through

technical solutions is more inline with the rise of industry groups such as the Microsoft Digital Crime Unit and various nongovernmental organizations to serve in crime prevention roles (Freilich & Newman, 2016; Holt & Bossler, 2016).

It is unknown at this time if industrial groups can engage in such enforcement activities without de-legitimizing the role of law enforcement to respond to cybercrime (Holt & Bossler, 2016; Hutchings & Holt, 2014), and/or if such efforts will encourage or enhance collaborative efforts between the police and private sector industry groups to prevent these crimes (Freilich & Newman, 2016). For instance, corporate cybersecurity vendors provide minimal statistics on hacking and malware incidents to the general public, and minimal information when a serious hack or compromise affects their customer base (Andress & Winterfeld, 2013; Brenner, 2009). They also give little insights on the extent to which their products are able to effectively prevent various forms of cyber-attack.

The existing lack of transparency may further hinder our knowledge of ideologically motivated cyberattacks. Similarly, the political nature of these attacks may lead an organization to see ideological cyberattacks as the government's domain, and not their responsibility, especially if the form of ideological extremism (global vs. homegrown, far-right vs. jihadist) is more far-reaching in scope. Future research is thus needed to understand the degree of public support for increased industrial engagement in ideological cyberattacks and the way that organizational responses are shaped by the nature of the attack (Holt & Bossler, 2016).

Additional study is also required to better understand the role of a mission or nationalist identity in the hacks performed by individuals across the globe. The notion of "the mission" differentiated Turkish hackers' perception of the hacker subculture from that of the larger norms identified in primarily Western nations established in prior research (e.g., Holt, 2007; Jordan & Taylor, 1998). It is possible that nationalism may emerge as a factor in other nations depending upon their preferred targets and relationships with neighboring nations, and the larger global community. The general absence of research on this issue, however, demands further inquiry to establish if this is a unique feature of the Turkish community, an artifact of the community as of the time of data collection, or an under-represented norm that is evident in some nations as a whole.

The limitations of this study's sample require further study to understand variations in the influence and experiences of ideologically motivated hackers generally. The data collection methods employed in this study did not allow for substantive follow-up with participants to gain additional insights on certain points. While all respondents could be contacted electronically for clarification, it was minimized for the sake of efficiency and expediency (see Holt, 2010). Additional methods to triangulate the data and findings, such as the use of participant observations in natural settings, may help improve the depth of this analysis (see Holt, 2007).

There is also a need for more research to understand the ways that differences in technological access by region may directly shape the experience of hackers and their general attack capabilities (Holt & Kilger, 2012). The substantive focus on Turkey limits the generalizability of these findings to other nations or hacker communities.

Interviewing hackers from various nations would provide direct insights into the ways that the hacker subculture is experienced and valued by place.

Similarly, an individual's ideological affiliation may directly shape their motivations and targets when hacking. The focus of this study on hackers motivated by religious beliefs may limit its applicability to other ideological perspectives. Greater research is needed to understand how a person's views on animal rights may lead them to differentially target vivisection clinics and furriers. Similarly, it is possible that White nationalists may be more interested in affecting targets on the basis of race or ethnicity (Holt & Bolden, 2014).

The temporal bounding of this data may limit its utility to understand contemporary ideological hacking. As cultural and religious norms change, it is plausible that the actions of hackers may shift in tandem. At the same time, several norms of the hacker subculture are still consistently reported in qualitative populations across place and time (e.g., Holt, 2007; Jordan & Taylor, 1998; Steinmetz, 2015). Thus, research is needed to identify the extent to which the contextual values of ideologically motivated hackers are consistently identified in various populations. Further study is needed to address this issue and help identify the contours of the experience of hacking, and inform our understanding of the relationship between ideologically motivated cyberattackers and physical terror and extremism generally.

It is also essential to explore how hacking and other cybercrimes are part of radicalization processes, terrorist group behaviors, and terrorist offending online or offline (Holt, 2012). For example, it is unknown if ideologically motivated hackers are linked episodically to other hackers or are part of a larger group that shares similar motivations. It is also unclear if such activities are a precursor to physical violence, or pursued independently.

Finally, there is no research identifying the duration of an individual's involvement in ideologically motivated hacking. That is, are individuals first interested in acquiring skills and understanding the hacker craft and later radicalize toward extreme ideologically thinking, or do they start as radicalized individuals and then seek such technologies to further a cause they are already committed and involved in? This study suggests some Turkish hackers collaborate to facilitate hacks, which is substantively different from the larger body of evidence on hacking. This highlights the need to better understanding how such hackers are different from the larger hacker population. Future research must understand hackers' commitment to and involvement in extremist movements. Such research will improve our understanding of terror activities online and offline.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Anderson, D. S., Fleizach, C., Savage, S., & Voelker, G. M. (2007). Spamscatter: Characterizing internet scam hosting infrastructure. In *Usenix security* (pp. 1-14). New York, NY: Association for Computer Machinery.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: Techniques, tactics, and tools for security practitioners* (2nd ed.). Waltham, MA: Syngress.

Bakier, A. H. (2007, June 29). Forum users improve electronic jihad technology. *Terrorism Focus*, *4*(20). Retrieved from https://jamestown.org/brief/forum-users-improve-electronic-jihad-technology/

Bakker, E. (2006). *Jihadi terrorists in Europe, their characteristics and the circumstances in which they joined the jihad: An exploratory study*. The Hague, The Netherlands: Clingendael Institute.

Blevins, K. R., & Holt, T. J. (2009). Examining the virtual subculture of johns. *Journal of Contemporary Ethnography*, *38*, 619-648.

Bloom, M. (2005). *Dying to kill: The allure of suicide terror*. Columbia, NY: Columbia University Press.

Borum, R. (2011a). Radicalization into Violent Extremism I: A review of social science theories. *Journal of Strategic Security*, *4*(4), 7-36.

Borum, R. (2011b). Radicalization into Violent Extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security*, *4*(4), 37-62.

Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state.* New York, NY: Oxford University Press.

Britz, M. T. (2015). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (Ed.), *Crime on-line: Correlates, causes, and context* (pp. 193-220). Raleigh, NC: Carolina Academic Press.

Canali, D., Balzarotti, D., & Francillon, A. (2013). The role of web hosting providers in detecting compromised websites. In *WWW'13 Proceedings of the 22nd International Conference on World Wide Web*, May 2013 (pp. 177-188). Rio de Janeiro, Brazil: Association for Computer Machinery.

Conway, M. (2006). Terrorism and the Internet: New media—New threat? *Parliamentary Affairs*, *59*, 283-298.

Corbin, J., & Strauss, A. (2007). *Basics of doing qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*, 160-175.

Denning, D. E. (2010). Cyber-conflict as an emergent social problem. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). Hershey, PA: IGI Global.

Dupont, B., Côté, A.-M., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime*, *17*, 129-151.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants.* In ACM Conference on Computer and Communications Security (pp. 375-388). New York, NY: Association for Computer Machinery.

Freilich, J. D., & Chermak, S. M. (2016, October). Patterns of U.S. Extremist Crime, 2012–2016. *Findings from the ECDB*. *Invited Presentation to START's Annual Conference, University of Maryland*, *College Park*.

Freilich, J. D., Chermak, S. M., Belli, R., Gruenewald, J., & Parkin, W. S. (2014). Introducing the United States Extremist Crime Database. *Terrorism and Political Violence*, *26*, 372-384.

Freilich, J. D., Chermak, S. M., & Gruenewald, J. (2015). The future of terrorism research: A review essay. *International Journal of Comparative and Applied Criminal Justice*, *39*, 353-369.

Freilich, J. D., Chermak, S. M., & Simone, J., Jr. (2009). Surveying American state police agencies about terrorism threats, terrorism sources, and terrorism definitions. *Terrorism and Political Violence*, *21*, 450-475.

Freilich, J. D., & Newman, G. R. (Guest Eds.). (2009). *Crime Prevention Studies. Vol. 25: Reducing terrorism through situational crime prevention*. Boulder, CO: Lynne Rienner.

Freilich, J. D., & Newman, G. R. (2016). Transforming piecemeal social engineering into "grand" crime prevention policy: Toward a new criminology of social control. *Journal of Criminal Law and Criminology*, *105*, 203-232.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston, MA: Addison-Wesley.

Gruenewald, J., Allison-Gruenewald, K., & Klein, B. R. (2015). Assessing the attractiveness and vulnerability of eco-terrorism targets: A situational crime prevention approach. *Studies in Conflict & Terrorism*, *38*, 433-455.

Hamm, M. (2007). *Terrorism as crime: From Oklahoma City to Al Qaeda and beyond*. New York: New York University Press.

Herbert, S. (1998). Police subculture reconsidered. *Criminology*, *36*, 343-370.

Hoffman, B. (1998). *Inside terrorism*. New York, NY: Columbia University Press.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*, 171-198.

Holt, T. J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review*, *28*, 466-481.

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*, *24*, 337-354.

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime*, *14*, 155-174.

Holt, T. J., & Bolden, M. S. (2014). Technological skills of white supremacists in an online forum: A qualitative examination. *International Journal of Cyber Criminology*, *8*, 79-93.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London, UK: Routledge.

Holt, T. J., Bossler, A. M., & Fitzgerald, S. (2010). Examining state and local law enforcement perceptions of computer crime. In T. J. Holt (Ed.), *Crime online: Correlates, causes, and context* (pp. 221-246). Raleigh, NC: Carolina Academic Press.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. London, England: Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). *Policing cybercrime and cyberterror*. Raleigh, NC: Carolina Academic Press.

Holt, T. J., & Kilger, M. (2012). Examining willingness to attack critical infrastructure on and off-line. *Crime & Delinquency*, *58*, 798-822.

Holt, T. J., Kilger, M., Chiang, L., & Yang, C. S. (2017). Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks. *Deviant Behavior*, *38*, 356-373. doi:10.1080/01639625.2016.1197008

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets on-line: Products and market forces. *Criminal Justice Studies*, *23*, 33-50.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*, 81-103.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*, 1163-1178.

Hutchings, A., & Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*, 596-614.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*, 757-780.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* London, UK: Psychology Press.

Kilger, M. (2010). Social dynamics and the future of technology-driven crime. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 205-227). Hershey, PA: IGI Global.

Krebs, B. (2007, July 6). Three worked the web to help terrorists. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945.html

Kunkle, J. (2012, June). Social media and the homegrown terrorist threat. *The Police Chief*, *79*, p. 22.

LaFree, G., & Dugan, L. (2007). Introducing the global terrorism database. *Terrorism and Political Violence*, *19*, 181-204.

Leyden, J. (2007, November 7). Scepticism over cyber-jihad rumours: Al-Qaeda (still) can't hack. *The Register*. Retrieved from https://www.theregister.co.uk/2007/11/02/cyber_jihad_rumours/

Loper, D. K. (2000). *The criminology of computer hackers: A qualitative and quantitative analysis* (Doctoral dissertation). Michigan State University, East Lansing.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*, 33-59.

Martin, G., & Augustus, C. C. (2016). *Essentials of terrorism: Concepts and controversies*. Los Angeles, CA: Sage.

McCauley, C., & Moskalenko, S. (2011). *Friction: How radicalization happens to them and us*. Oxford, UK: Oxford University Press.

Meyer, G. (1989). *The social organization of the computer underground* (Unpublished master's thesis). Retrieved from http://www.g2meyer.com/cu/computerunderground.pdf

Monahan, J. (2012). The individual risk assessment of terrorism. *Psychology, Public Policy, and Law*, *18*, 167-205.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 71-80). New York, NY: Association for Computing Machinery.

Newman, G. R., & Clarke, R. V. (2003). Superhighway robbery: Preventing e-commerce crime. New York, NY: Routledge.

Perez, E., Shoichet, C. E., & Bruer, W. (2015, October 19). Hacker who allegedly passed U.S. military data to ISIS arrested in Malaysia. *CNN*. Retrieved from http://www.cnn.com/2015/10/15/politics/malaysian-hacker-isis-military-data/

Pool, J. (2005, October 11). *Technology and security discussions on the jihadist forums*. Washington, DC: Jamestown Foundation.

Sageman, M. (2004). *Understanding terror networks*. Philadelphia: University of Pennsylvania Press.

Silber, M. D. (2011). *The Al Qaeda factor: Plots against the West*. Philadelphia: University of Pennsylvania Press.

Silverman, D. (2013). *Doing qualitative research: A practical handbook.* Thousand Oaks, CA: Sage.
Simi, P., & Futrell, R. (2010). *American swastika: Inside the White power movement's hidden spaces of hate*. New York, NY: Rowman & Littlefield.
Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology*, 55, 125-145.
Stern, J. (2003). *Terror in the name of God: Why religious militants kill*. New York, NY: HarperCollins.
Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. New York, NY: Routledge.
Thomas, D. (2002). *Hacker culture*. Minneapolis: University of Minnesota Press.
Torres-Soriano, M. R. (2016). The hidden face of jihadist internet forum management: The case of Ansar Al Mujahideen. *Terrorism and Political Violence*, *28*, 735-749.
Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, *2*, 382-396.
Ulph, S. (2006, February 7). Internet mujahideen refine electronic warfare tactics. *Terrorism Focus*, *3*(5). Retrieved from https://jamestown.org/program/internet-mujahideen-refine-electronic-warfare-tactics/
Ward, M. (2006, February 8). Anti-cartoon protests go online. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/technology/4692518.stm
Weinberg, L., Pedhazur, A., & Hirsch-Hoefler, S. (2004). The challenges of conceptualizing terrorism. *Terrorism and Political Violence*, *16*, 777-794.
Woo, H., Kim, Y., & Dominick, J. (2004). Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology*, *6*, 63-82.
Zone-H.org. (2016). *Stats*. Retrieved from http://www.zone-h.org/stats

Author Biographies

Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University specializing in cybercrime, policing, and policy. He received his PhD in Criminology and Criminal Justice from the University of Missouri-Saint Louis in 2005. He has published extensively on cybercrime and cyberterror in outlets such as *Crime and Delinquency, Deviant Behavior, Journal of Criminal Justice, Sexual Abuse*, and *Terrorism and Political Violence.*

Joshua D. Freilich is a member of the Criminal Justice Department and the Criminal Justice PhD Program at John Jay College. He is the creator and co-director of the United States Extremist Crime Database (ECDB), an open source relational database of violent and financial crimes committed by political extremists in the United States. His research has been funded by the Department of Homeland Security (DHS) and the National Institute of Justice (NIJ). His research focuses on the causes of and responses to terrorism, bias crimes, measurement issues, and criminology theory, especially environmental criminology and crime prevention.

Steven M. Chermak is a professor in the School of Criminal Justice at the Michigan State University, an investigator for the National Consortium for the Study of Terrorism and Responses to Terrorism, and creator and co-director of the United States Extremist Crime Database (ECDB). He studies domestic terrorism, media coverage of crime and justice issues, and the effectiveness of specific policing strategies. Recent publications have appeared in *Terrorism and Political Violence, Crime and Delinquency*, and *Journal of Quantitative Criminology*.